ECE 404 Homework #10

Due: Thursday 4/4/2019 before class

Buffer Overflow Attacks

In the Homework section of the course webpage, you will find two socket programs written in C. One of them acts as a server and the other as a client. Your task is to launch an attack such that you execute the "secret" function in the server side code by using the client program to send a carefully crafted string to the server. *Then*, show how you would fix server.c to prevent such a buffer overflow attack.

- If using gcc on your Linux machine, compile the server and client programs with the '-fno-stack-protector' option. Refer to pages 36-37 of Lecture 21 for more details. If you wish, you can also use the Tiny C compiler tcc that can be used without options.

- You can test the programs with two different shell terminals: one terminal for a server and the other terminal for a client. You can also run the server on a Purdue ECN machine using a high numbered port like 7777 and the client on your own laptop.

- Use gdb to determine how you can develop a string to send (using the client program) to the server program and trigger the execution of `secretFunction()`. Refer to lecture 21.6 for more details on how to do this. Here are some things to keep in mind when creating this string:

  1. While you send the data with the client program, you will have to run the server program with gdb to determine the buffer overflow string to use.
  2. When sending the string to the server program, note that you can send ASCII characters as well as hexadecimal-format bytes. You can send, for example, the hex byte `0xAD` using the format `\xAD`.
  3. As in the lecture notes, you will need to reverse the order of addresses sent to deal with big endian-little endian conversion problems.

- After you have crafted your buffer overflow string and triggered the execution of `secretFunction()`, modify server.c to remove the buffer overflow vulnerability. Include comments in the code explaining what the vulnerability was and how you fixed it.

Submission Notes

- The hard-copy submission must include the specially-crafted buffer overflow string, an explanation of why you chose the string, the modified server code, and an explanation of your fixes to the code as detailed above. Please indicate the modified parts of the server code by highlighting or underlining them.

- The electronic submission should include the modified server code with explanation in the comments.

- As always, the submitted file should include a Homework Header as described in the homework section of the ECE 404 website.

Electronic Turn-in

```
turnin -c ece404 -p hw10 new_server.c
```